امحاء تجهیزات کامپیوتری

تهیه و تنظیم: اسماعیل اللهیار

دسترسی‌ها را حذف کنید

اطمینان حاصل کنید که تمامی حساب‌های کاربری یا سایر امکانات کنترل دسترسی مرتبط با تجهیزاتی که قرار است دور بیندازید، حذف شده‌اند. قطعاً شما نمی‌خواهید که کارمند اخراجی سازمان، همچنان به دستگاه خود دسترسی داشته باشد و قطعاً مایل نیستید که حساب‌های کاربری بلا استفاده شبکه که دیگر موردنیاز نیستند، برای اتصال از راه دور مورد استفاده قرار گیرند و امکان حمله را افزایش دهند. پیش از هر کاری باید این مرحله را انجام دهید.

داده‌ها را تخریب کنید

به هیچ عنوان تصور نکنید که دور انداختن یک درایو سخت از لحاظ امنیتی کافی است. در صورتی که داده‌های حساسی بر روی درایوهای شما وجود دارد، باید پیش از دور انداختن دیسک سخت از شر این داده‌ها خلاص شوید. حتی اگر تصور نمی‌کنید که داده حساسی بر روی درایوها وجود داشته باشد، باز هم بر روی تجارت خود قمار نکنید. حتی فرمت کردن یا پارتیشن‌بندی مجدد درایو یا حذف داده‌های آن نیز کافی نیست.

دستگاه را تخریب کنید

در برخی موارد لازم است که تجهیزات ذخیره‌سازی به‌طور فیزیکی تخریب شوند تا اطمینان حاصل شود که داده‌های حساس نشت نخواهند یافت. در این شرایط احتمالاً نباید خود شما این کار را انجام دهید. بلکه متخصصینی وجود دارند که این کار را برای شما انجام می‌دهند و به شکل بسیار مطمئن‌تری داده‌های شما را غیر قابل بازیابی خواهند ساخت. در صورتی که سیاست‌های سازمان شما اجازه سپردن این کار را به گروهی خارج از سازمان نمی‌دهد، باید گروهی متخصص و با تجهیزات لازم برای این کار در درون سازمان خود داشته باشید.

روش‌مند باشید

یک چک‌لیست برای فرآیند دور انداختن تجهیزات خود داشته باشید تا مطمئن باشید که هیچ گامی را فراموش نخواهید کرد. این مسئله به‌خصوص زمانی که قصد دارید تجهیزات زیادی را دور بیندازید، از اهمیت ویژه‌ای برخوردار خواهد بود، اما در حالت عادی نیز مهم است که از این روش پیروی کنید. البته انتظار نداشته باشید که چک‌لیست شما به جای شما فکر کند. تک‌تک جزئیات سیستم مورد نظر، استفاده‌های آن و هر خطر بالقوه امنیتی را در نظر بگیرید. زمانی‌که با تهدید جدیدی روبه‌رو می‌شوید که ممکن است در آینده نیز با آن برخورد کنید، معیاری جدید را به چک‌لیست خود اضافه کنید. به خاطر داشته باشید که لازم نیست تک‌تک عناصر این چک‌لیست در تمامی موارد مورد استفاده قرار گیرند.

سیستم‌هایی را که دور انداخته شده‌اند ره‌گیری کنید

اطمینان حاصل کنید که نشانه‌های فیزیکی روشنی از پاکسازی کامل یک سیستم به روشی کاملاً امن در اختیار دارید و اطمینان حاصل کنید که چیزی اشتباه نشده است. بهتر است کامپیوترهایی که کاملاً پاکسازی نشده‌اند در مکان خاصی نگهداری شوند و سیستم‌هایی که کار پاکسازی آنها کامل شده است در مکانی دیگر قرار گیرند تا از ایجاد اشتباه جلوگیری شود. این کار احساس فوریت نیاز به پاکسازی امن تجهیزات را نیز افزایش می‌دهد.

همه چیز را با دقت ثبت کنید

هرکس که مسئول دور انداختن یک سیستم باشد باید اتمام کار پاکسازی و دور انداختن سیستم را امضا کند. در صورتی که چند نفر مسئول این کار باشند نیز باید مسئولیت هر فرد به دقت مشخص شده و اتمام کار نیز امضا شود. در این صورت اگر مشکلی پیش بیاید، شما می‌دانید که با چه کسی صحبت کنید. زمان و تاریخ اتمام کار نیز باید ثبت شود. همه چیز از جمله ویژگی‌های تجهیزات، مکانی که به آن انتقال داده خواهند شد، هزینه استهلاک و هزینه جایگزینی آنها را با دقت ثبت کنید.

منتظر نمانید

زمانی که تصمیم می‌گیرید سیستمی را دور بیندازید، معطل نکنید. هرچه سریع‌تر کار پاکسازی کامل آن را انجام داده و کار را تمام کنید. اجازه ندهید این کار برای هفته‌ها، ماه‌ها یا سال‌ها مورد غفلت قرار گیرد تا کسی نتواند از داده‌های موجود بر روی آن سیستم سوءاستفاده کند. علاوه بر آن اگر

به سیستمی احتیاج ندارید، اجازه ندهید همچنان بر روی شبکه شما در حال کار باشد تا راهی برای نفوذ خرابکاران ایجاد کند.

شواهد بالقوه را حذف کنید

تنظیمات پیکربندی تجهیزات شبکه‌ای را پاک کنید. سوئیچ‌های مدیریت شده، سرورهای احراز هویت و سایر تجهیزات زیرساخت شبکه هوشمند می‌توانند شواهدی را در اختیار یک مجرم رایانه‌ای قرار دهند تا راحت‌تر به شبکه شما و سیستم‌های آن نفوذ کند.

سیستم‌ها را تا زمان دور انداختن امن نگه دارید

راهکارهای روشنی را تدوین کنید تا مشخص شود چه کسانی اجازه دسترسی به کدام تجهیزات دور انداختنی را دارند. این کار باعث می‌شود که هیچ فرد غیر مجازی پیش از پاکسازی کامل یک دستگاه، به آن دسترسی پیدا نکند.

از تمامی تجهیزات فهرست‌برداری کنید

محتویات فیزیکی هر سیستم و هریک از تجهیزات شبکه سازمان خود را ردیابی کنید تا چیزی از نظر دور نماند. به خاطر داشته باشید که حتی RAM نیز در شرایط خاص می‌تواند به‌عنوان ابزار ذخیره‌سازی داده‌های حساس محسوب شود. باید در مورد داده‌های حساس با وسواس و دقت تمام رفتار کنید.

نباید دقت و وسواس زیاد در امن‌سازی سیستم‌های در حال استفاده، شما را از امنیت سیستم‌هایی که می‌خواهید دور بیندازید غافل کند. دور انداختن یک کامپیوتر، به معنای عدم نیاز به امن‌سازی آن نیست.